UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI

MARITZ HOLDINGS INC., Plaintiff, v. COGNIZANT TECHNOLOGY SOLUTIONS U.S. CORPORATION, Defendant.	Case No. 4:18-cv-00826-CDP

COGNIZANT'S REPLY MEMORANDUM IN FURTHER SUPPORT OF ITS MOTION TO DISMISS MARITZ' COMPLAINT FOR FAILURE TO STATE A CLAIM UPON WHICH RELIEF CAN BE GRANTED

Ronald J. Tenpas (admitted *pro hac vice*)
VINSON & ELKINS
2200 Pennsylvania Ave. NW
Suite 500 West
Washington, DC 20037
Phone: (202) 639-6791
Fax: (202) 879-8981
rtenpas@velaw.com

Jim Martin
DOWD BENNETT
7733 Forsyth Blvd
St. Louis, MO 63105
Phone: (314) 889-7300
Fax: (314) 863-2111
jmartin@dowdbennett.com

-and-

Patrick A. Harvey (admitted *pro hac vice*)
MORGAN, LEWIS & BOCKIUS LLP
1111 Pennsylvania Avenue, NW
Washington, DC 20004
Phone: (202) 739-3000
Fax: (202) 739-3001
patrick.harvey@morganlewis.com

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

INTRODUCTION

Maritz sued Cognizant, alleging Maritz suffered significant losses from phishing attacks committed by an admittedly "unidentified perpetrator." ECF No. 1 ("Compl.") ¶ 28. Cognizant moved to dismiss Maritz' Complaint in its entirety because the Complaint failed to state a plausible claim that Cognizant was responsible for either the attacks or Maritz' economic losses. Unable to plead facts plausibly indicating that unidentified Cognizant employees improperly accessed Maritz' network to steal eGift Cards on Maritz' computer systems (Compl. ¶¶ 50, 60), Maritz asks the Court simply to *infer* that "Cognizant employees hacked Maritz' computer system and are responsible for over $12 million in losses sustained by Maritz from the attacks." ECF No. 28 ("Maritz Mem.") 2. Such an implausible inference is barred by *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007) and *Ashcroft v. Iqbal*, 556 U.S. 662 (2009).

Maritz alleges no facts directly linking Cognizant to the first attack in 2016. For the separate 2017 attack, Maritz claims that "the attackers were accessing the Maritz system using accounts registered to Cognizant." Compl. ¶ 43. That allegation is wholly insufficient because Maritz concedes that *its own employees* succumbed to phishing attacks in February 2017, which led to hackers stealing eGift Cards from Maritz's systems. *Id.* ¶ 39. According to the Complaint, the only time Cognizant accounts were allegedly used to access the Maritz system was two months later in April 2017—*after* Maritz installed "cyber protections" (*id.*) following the February 2017 theft caused by its employees' failure to appropriately respond to phishing attacks (*id.* ¶¶ 39–40). In other words, Maritz is trying to pin both the 2016 and 2017 thefts on Cognizant even though not a single Cognizant account is alleged to have been used until months after the later 2017 attack occurred, and even though Maritz admits that its own employees let the hackers access its system.

The mere fact that Cognizant accounts were allegedly used in April 2017 cannot salvage Maritz' Complaint. There are many ways that accounts registered to Cognizant may have been

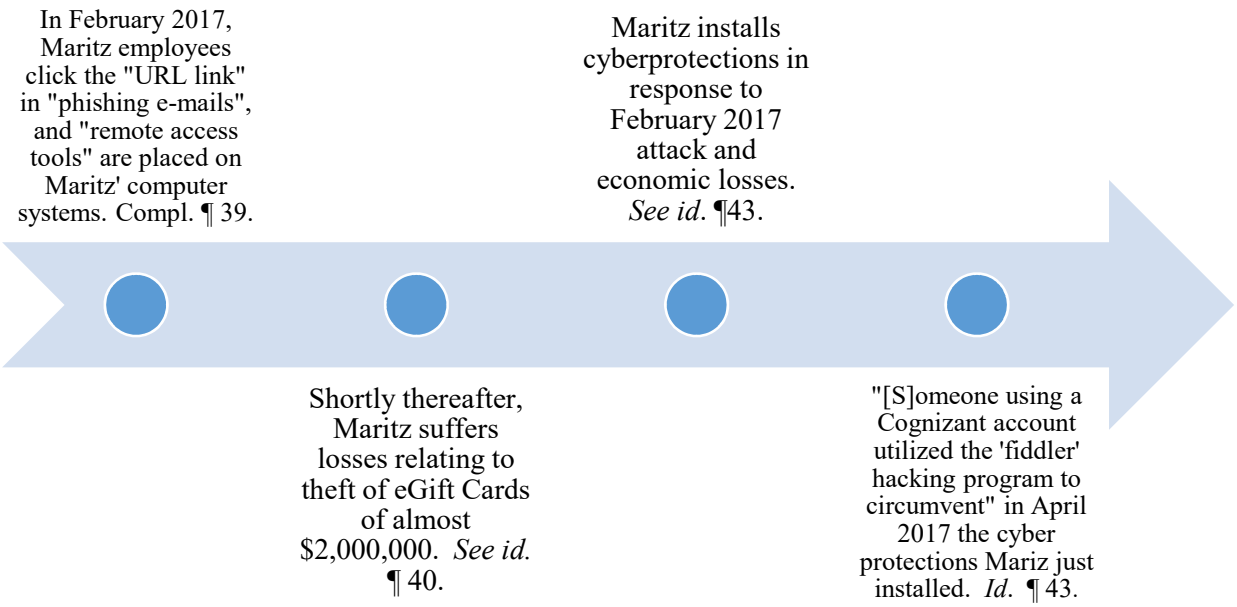
used without the involvement of any Cognizant employees. For example, Maritz admits that in 2016 the perpetrator successfully harvested Maritz' Access Directory credentials—*i.e.*, a complete list of logins and passwords used to access the Maritz' computer system. That hacker thus could have used this stolen information to login with accounts linked to Cognizant in 2017. Moreover, the very nature of the 2017 phishing attack alleged by Maritz—in which "Maritz employees" accessed a "URL link" in "spear phishing emails" that maliciously installed "remote access tools" giving the "perpetrator(s) broad access to Maritz'[] computer systems" (Compl. ¶ 39)—strongly implies that Cognizant accounts were compromised during the phishing attack. Maritz must allege something more to make its claim plausible when there is an "obvious alternative explanation" for a defendant's conduct, *Iqbal*, 556 U.S. at 682, and there are many reasons why Cognizant accounts may have been used after the 2016 and 2017 attacks had been completed.

Finally, even if these fundamental failures, fatal to all of its claims, are overlooked, Maritz still fails to show that vicarious liability can support its statutory or tort claims, that Cognizant breached the Master Services Agreement ("MSA"), or that Maritz has stated a valid claim for negligence, unjust enrichment, or equitable accounting. Thus, each of Maritz' claims fail in multiple ways, and accordingly, Maritz' Complaint should be dismissed with prejudice.

ARGUMENT

I. Maritz Cannot Rely on Conclusory Allegations to Support an Inference That a Cognizant Employee Participated in the 2017 Phishing Attack.

In requesting an inference that Cognizant employees participated in a 2017 phishing attack, Maritz claims that it "alleged that Cognizant employees using accounts assigned to Cognizant stole millions from its computer system." Maritz Mem. 5 (emphasis removed). Not so. Maritz' pleading simply does not make that allegation. In fact, it alleges as follows:



The upshot is that, after an investigation allegedly costing Maritz over $5M (Compl. ¶ 41), Maritz only alleges that Cognizant accounts may have been used to attempt to work around security defenses *after* the theft was completed and *after* Maritz attempted to construct additional cyber protections in response to that theft. Then, and only then, someone used a Cognizant account to attempt to bypass the new cyber protections using the "fiddler" program. *Id.* ¶ 43. Thus, Maritz's foundational argument—that the perpetrator used Cognizant accounts *to steal from Maritz* in 2017—is wholly unsupported by its factual allegations in the Complaint.

Under the allegations actually included in the Complaint, the path to Cognizant employee involvement is implausible. First, a Cognizant employee allegedly stole over $12 million in conjunction with two separate phishing attacks nearly a year apart, presumably conducting those phishing attacks (and not logging in with his/her credentials) in order to evade detection. Then, after Maritz detected the attack and installed additional cybersecurity, that same employee decided not to conduct another phishing attack. Rather, he/she decided to announce his/her presence by logging into Maritz's system with his/her Cognizant account for the sole purpose of evading those security measures; but then decided not to steal anything afterwards. The Court cannot infer such

an unreasonable chain of events to save Maritz' Complaint. *E.g.*, *Hiland Dairy, Inc. v. Kroger Co.*, 402 F.2d 968, 973 (8th Cir. 1968) (court cannot make "unreasonable inferences or unwarranted deductions of fact" when ruling on a motion to dismiss).

In all events, the use of Cognizant accounts after the February 2017 theft does not make it reasonable to infer that Cognizant employees participated in the earlier phishing attack(s). Maritz alleges it suffered two phishing attacks, one in 2016 and one in 2017. A phishing attack attempts "to acquire information such as usernames, passwords, or financial data" by tricking the victim of the attack "to enter or update personal information at the phony website" in order to gain that personal information." *Choice Escrow & Land Title, LLC v. BancorpSouth Bank*, 754 F.3d 611, 615 n.2 (8th Cir. 2014). As Maritz admits, an attack in 2016 succeeded in *compromising credentials used to gain access to working on the Maritz computer systems*. That is the cyber equivalent of getting keys to the front door.[1] Thus, the 2016 hackers had the credential information that Cognizant employees used to access Maritz' system. Nor does Maritz allege that it did anything to address this problem after the 2016 attack (such as issuing new credentials, or resetting the Active Directory). Maritz also did not even give Cognizant notice of the 2016 attack. Thus, on Maritz' own pleaded allegations, the perpetrators of a successful phishing attack had, from 2016 onward, access to Cognizant's login credentials. On top of that, Maritz acknowledges that the 2017 attack involved further phishing attack efforts. According to Maritz, the 2017 attackers used "spear phishing or targeted emails" that planted "remote access tools" that "permitted the perpetrator(s) broad access to Maritz's computer systems." Compl. ¶ 39. Thus, on Maritz' own

[1] Specifically, as Maritz acknowledges, the first 2016 attack resulted in malware being installed that could "harvest active directory credentials." Compl. ¶ 28. Active Directory is a "software product sold by Microsoft that is used to, among other things, authenticate software users." *Apacheta Corp. v. Lincare, Inc.*, No. CV 16-2030, 2018 WL 3831377, at *9 (E.D. Pa. Aug. 13, 2018). It is a tool used to track and manage credentials and access to computer systems. *See id.*

allegations, by 2017 Maritz's system had a second vulnerability to external attacks: remote access by hackers.

These factual allegations belie any inference that Cognizant employees were involved in either attack. First, both the 2016 and 2017 attacks came through "phishing"— i.e., efforts to break through and secure access to the Maritz systems by someone who did not already have access—the cyber equivalent of someone breaking through a window because he lacks the key. Not only could such phishing be conducted by anyone in the world, a Cognizant employee, who already had access credentials, would have less need to take this approach than someone without access credentials. Second, as to the use of a Cognizant account in April 2017, the compromise of Maritz' credential system in 2016 means that anyone associated with that 2016 hack (or a recipient of such information) could have used any Cognizant employee's login credentials thereafter.

Maritz offers little in response. Maritz asks the Court "to infer that whoever used the Cognizant accounts to steal from Maritz in 2017" must have been "involved with the phishing attacks" because they allegedly knew about the "malicious files" planted through the phishing attacks committed by an "unidentified perpetrator." Maritz Mem. 4. As an initial matter, Maritz again misstates the factual allegations in the Complaint. As explained above, the Complaint does not plead that any Cognizant accounts were used "to steal from Maritz in 2017"; rather, it alleges the use of a Cognizant account in April 2017 after the thefts allegedly occurred in February 2017. In all events, Maritz simply has not pleaded facts plausibly showing, as they must, that "whoever used the Cognizant accounts" in April 2017 *were Cognizant employees*. Merely suggesting that whoever used the Cognizant account in April 2017 *might* have been the same person who conducted the earlier phishing attack(s) does nothing to indicate who that person was. It is implausible to conclude that it was a Cognizant employee because: (a) a Cognizant employee with

credentials to access the Maritz system is an unlikely candidate to engage in phishing, unless he or she wanted to cover his or her tracks; (b) if a Cognizant employee wanted to cover his or her tracks by conducting a phishing attack, he or she would not then decide to use a Cognizant accounts to engage in additional hacking; (c) the attacks in 2016 gave hackers access to Cognizant employee credentials; and (d) Maritz does not allege that it took security measures to ensure that the 2016 perpetrator could not use Cognizant's access credentials in April 2017.[2]

Because Maritz permitted Cognizant accounts to be comprised in 2016 and 2017 – without any notice whatsoever to Cognizant—it is highly likely that perpetrator(s) unaffiliated with Cognizant "were accessing the Maritz system using accounts registered to Cognizant." Compl. ¶ 43. This more logical alternative precludes an inference of Cognizant employee wrongdoing because "[a]n inference pressed by the plaintiff is not plausible if the facts [it] points to are precisely the result one would expect from lawful conduct in which the defendant is known to have engaged." *Braden v. Wal-Mart Stores, Inc.*, 588 F.3d 585, 597 (8th Cir. 2009). In this instance where "there is a concrete, 'obvious alternative explanation'" for who was using the Cognizant employee credentials, Maritz should "be required to plead additional facts tending to rule out the alternative." *Id.* (quoting *Iqbal*, 556 U.S. at 682).[3] It cannot do so.

II. Inferring Cognizant Was Involved in the 2016 Attack Is Unreasonable.

In its Motion to Dismiss, Cognizant argued (at 4) that allegations describing the 2016 attack must be disregarded because no allegations directly link Cognizant employees to the attack. In

[2] Maritz claims this question presents a "chicken and egg" argument. Maritz Mem. 5 n.3. Not so. The phishing attacks and the compromise of the active directory indisputably came before any eGift Cards were stolen.

[3] Citing a case from the Ninth Circuit, Maritz argues that "the Court must accept Maritz' theory [that Cognizant employees stole the eGift Cards] at this stage." Maritz Mem. 5. But even using the Ninth Circuit standard, Maritz only gets that benefit if its theory is plausible. *See Starr v. Baca*, 652 F.3d 1202, 1216 (9th Cir. 2011) ("If there are two alternative explanations, one advanced by defendant and the other advanced by plaintiff, *both of which are plausible* . . ." (emphasis added)). As explained in this section, Maritz has not demonstrated plausibility.

response, Maritz does not claim that it has directly alleged, or could directly allege under Rule 11, that Cognizant participated in the 2016 phishing attack. Instead, Maritz asks the Court to jump to yet another unjustified inference. *See* Maritz Mem. 3.

As explained above, the Court cannot assume that Cognizant employees were involved in the 2017 phishing attack. *Supra* at I. But even if such an inference were appropriate, there is no basis to infer further that Cognizant employees were behind the earlier 2016 phishing attack. Any such claim is based on nothing more than the allegation that both attacks appear similar. *See* Compl. ¶¶ 42–43. But they're not similar. The 2017 attacks allegedly involved the use of Cognizant accounts, which is not alleged to be part of the 2016 attack. Claiming that the attacks were *otherwise* similar does not "nudge[]" Maritz' claim "across the line from conceivable to plausible." *Twombly*, 550 U.S. at 570 and 562 (allegations that leave open only an event's "sheer possibility" are insufficient). Notice pleading "does not unlock the doors of discovery" for plaintiffs like Maritz "armed with nothing more than conclusions" and appeals for unreasonable inferences. *Iqbal*, 556 U.S. at 678–79.

In sum, Maritz asks the Court to infer that Cognizant employees participated in the 2017 thefts, where Maritz employees succumbed to phishing attacks; and then to use that inference as the basis for another inference that Cognizant employees participated in the 2016 attack. There is no dispute that anyone in the world can launch a phishing attack from anywhere in the world. Each inference is unreasonable on its own. But combined, the multiple inferences that Maritz seeks stretch further and further away from plausibility. *See In re Merrill Lynch Auction Rate Sec. Litig.*, 886 F. Supp. 2d 340, 344 (S.D.N.Y. 2012) (piling "inference upon inference" stops "short of the line between possibility and plausibility of entitlement to relief."). The Court should decline to "make inference upon inferences to provide the factual enhancement" to save Maritz' claim that

Cognizant employees participated in the attack. *Mitchell v. Proctor & Gamble*, No. 2:09-CV-426, 2010 WL 728222, at *5 (S.D. Ohio Mar. 1, 2010).

III. *Respondeat Superior* Cannot Save Maritz' CFAA, MCTS, and Conversion Claims.

Maritz disputes the proper vicarious liability standards for its Computer Fraud and Abuse Act ("CFAA"), Missouri Computer Tampering Statutes ("MCTS"), and conversion claims. Its claims lack merit.

Nearly every federal court to consider vicarious CFAA legal liability has concluded that an employer must have, for its own benefit, affirmatively "urged," "induced," "encouraged," or "directed" wrongful conduct. *See* ECF No. 17 ("Cognizant Mem.") 7. Against this wave of authority, Maritz offers a single, unpublished, 15-year-old decision from a district court in Virginia, *Physicians Interactive v. Lathian Systems, Inc*., No. 03-1193-A, 2003 WL 23018270 (E.D. Va. Dec. 5, 2003). *See* Maritz Mem. 6. That case is an inapposite outlier. The *Physicians Interactive* court never even considered the issue on a contested basis because the *defendant* (without opposition from the plaintiff) in that case argued that Virginia's *respondeat superior* principles applied. 2003 WL 23018270, at *9–*10. Thus, the well-reasoned CFAA liability principles articulated in all other federal courts should control here. Because Maritz has not met those well-settled standards, Maritz' CFAA claim cannot survive.

To the extent Missouri *respondeat superior* principles apply to Maritz' statutory or conversion claims, they still fail. Maritz argues that Cognizant should be vicariously liable because the theft occurred while a Cognizant employee was "performing services under the [MSA]." Maritz Mem. 8. But that alone cannot trigger vicarious liability. Otherwise, any employer would be on the hook for any employee tort committed during business hours. That is not the law. Indeed, Missouri law makes clear that certain employee acts are not within the scope of employment even when they are committed while working. *See, e.g., Inman v. Dominguez*, 371

S.W.3d 921, 926 (Mo. Ct. App. 2012) (truck driver's stabbing of another driver is outside his employment scope even though the attack took place while the driver was en route to transporting his employer's goods); *P.S. v. Psychiatric Coverage, Ltd.*, 887 S.W.2d 622, 625 (Mo. Ct. App. 1994) (therapist's repeated sexual encounters with a patient fell outside his clinic employment scope even though some encounters occurred at the clinic during business hours).

Consequently, it is not sufficient under Missouri law to allege that the theft and hacking naturally arose from Cognizant employees' performance under the contract. *See* Maritz Mem. 8. Employers can only be vicariously liable for employee "acts (1) which, even though not specifically authorized, are done to further the business or interests of the employer under his general authority and direction *and* (2) which naturally arise from the performance of the employer's work." *Daugherty v. Allee's Sports Bar & Grill*, 260 S.W.3d 869, 872–73 (Mo. Ct. App. 2008) (emphasis added) (citations omitted). Maritz incorrectly claims that only one of these factors is required, when in fact both are.

Maritz has pleaded no facts to meet either factor, let alone both of them. An act "naturally" arises from work *when it is reasonable for an employer to foresee* that an employee would perform the tortious act during his employment. *See Daugherty*, 260 S.W.3d at 872–73. But "serious crimes are not only unexpectable but in general are in nature different from what servants in a lawful occupation are expected to do." *Wellman v. Pacer Oil Co.*, 504 S.W.2d 55, 58 (Mo. banc 1973) (quoting Restatement (Second) of Agency § 231, cmt a). These serious crimes "arise wholly from some external, independent or personal motive" and cannot arise from the employer's work as a matter of law. *Daugherty*, 260 S.W.3d at 872–73. On the other hand, an employer may face vicarious liability for more predictable minor offenses. *See id.* (employer potentially can be

vicariously liable for a practical joke gone awry—bartender placing a toothpick in a fellow employee's beer).

Here, Maritz alleges a multi-millions dollar theft, a class C felony punishable by between five and fifteen years in prison. MO. ANN. STAT. § 570.030; MO. ANN. STAT. § 558.011. It's not a practical joke. Cognizant could have never foreseen that its employees would participate in a theft of that scale (indeed, as described above, there is no factual basis to conclude that they did). *See Island Associated Coop. Inc. v. Hartmann*, 118 A.D. 2d 830, 831 (N.Y. App. Div. 1986) (rejecting *respondeat superior* for conversion claim); *Leafgreen v. Am. Family Mut. Ins. Co.*, 393 N.W.2d 275, 281 (S.D. 1986) (same).[4] Nor is there any allegation that, even if the Cognizant employees were behind the attack, that the attack was to Cognizant's benefit. Accordingly, even if Maritz has alleged facts to make it plausible that a Cognizant employee stole eGift Cards, Maritz' CFAA, MCTS, and conversion claims still fail both prongs for imposing *respondeat* liability.[5]

IV. Maritz Still Has Not Alleged a Breach of Any Contractual Provision in the MSA.

Maritz largely ignores Cognizant's arguments for dismissing Maritz' four distinct contract breach theories. They should be dismissed.

A. Preventing Third-Parties from Accessing Maritz' Computer Data for Improper Services.

Maritz admits that Cognizant did not explicitly promise to prevent unauthorized personnel access to Maritz' systems. Maritz Mem. 9. But Maritz ignores the contract's disclaimer of additional warranties and representations not expressly included in the contract. Cognizant

[4] In its opening brief, Cognizant argued that Maritz did not plausibly allege facts that Cognizant negligently hired any employees. Cognizant Mem. 10. Maritz' opposition ignores that argument entirely and thereby concedes the point. *See Thomas v. Walmart Stores, LLP,* No. 4:13CV00565 HEA, 2014 WL 117645, at *2 (E.D. Mo. Jan. 13, 2014).

[5] Maritz argues that it does not need to allege that Cognizant "acted with wrongful motive or intent." Maritz Mem. 7 n.3. But this does not mean that conversion is still not an intentional tort, because Maritz must still allege that Cognizant "intended to do an act which deprived [it] of [its] property." *Hinton v. State Farm Mut. Auto. Ins. Co.*, 741 S.W.2d 696, 699 (Mo. Ct. App. 1987).

Mem. 11. Cognizant, which was never hired to provide cybersecurity services for Maritz, never promised it would prevent third-parties from accessing Maritz' computer network.

B. Failing to Prevent Its Employees from Sharing Credentials and Usernames.

Maritz' opposition does not identify a contractual provision prohibiting Cognizant employees from internally sharing credentials *amongst themselves*. Maritz points to § 9.1, in which both parties promise not to "use the Confidential Information of the other party for any purpose whatsoever except as expressly contemplated under this Agreement or any Statement of Work." But credentials do not fall within the definition of "Confidential Information," which is defined as "all information and proprietary materials, not generally known in the relevant trade or industry," MSA § 1.1, and are not included among the numerous listed examples. *See id.* Thus, Maritz has not sufficiently pleaded that Cognizant actually used any "Confidential Information."

Even if the internal sharing of credentials among Cognizant employees who were all authorized to access Maritz' systems violated the MSA (which it did not), Maritz has not plausibly alleged that such sharing *caused* the breach and Maritz alleged damages. Maritz argues that it alleged Cognizant employees shared credentials, and that the "shared information was used to hack the Maritz system in 2017." Maritz Mem. 10. Again, that misstates the allegations in the Complaint. What Maritz actually alleged was that a Cognizant account, which Maritz does not identify or further specify, "was used to hack the Maritz system in [April] 2017." Compl. ¶ 45; *Morgan Distrib. Co., Inc. v. Unidynamic Corp.*, 868 F.2d 992, 995 (8th Cir. 1989) ("[I]t is axiomatic that a complaint may not be amended by the briefs in opposition to a motion to dismiss."). There is no allegation that shared credentials were in any way related to that April 2017 use. Moreover, it is implausible to conclude that shared credentials were the cause of any problem given the phishing attacks that Maritz allegedly suffered in 2016 and 2017, as the whole point of a phishing attack is to obtain credentials that were not otherwise available (e.g., by

sharing). *See supra* I. Thus, Maritz's claim of breach associated with alleged credential sharing must be dismissed.[6]

C. Failing to "Take Responsibility" for Security Breaches.

Maritz does not explain what it means to fail to "take responsibility" for alleged security breaches, or which contractual provision gives rise to such an amorphous duty. Nor does Maritz explain what "take responsibility" could mean besides indemnification. *See* Cognizant Mem. 12–13; MSA §§ 11.1–11.1.4, 14.2. The disclaimer of any additional indemnifications beyond those expressly acknowledged in the MSA bars any claim that Cognizant had to "take responsibility" for security breaches. Maritz offers no basis to conclude otherwise.

All Maritz offers in opposition is an excerpt from the "Facilities and Safety and Security" section of the MSA. *Id.* § 6.2.2. In that section, Cognizant agreed that it "shall be responsible for and shall immediately notify Maritz of, investigate and remedy any security breaches or potential security breaches at the Service Location(s)." *Id.* Service Locations are defined as *physical* locations in India. Id. at § 6.1.1. Thus, this provision is about making sure Cognizant's physical premises were secure. It has no bearing to a cyberattack, much less one on Maritz's system. Moreover, Maritz does not allege (because it cannot) that it informed Cognizant of any security breach while the attack was ongoing. Maritz also did not inform Cognizant of the alleged phishing attacks until well after they had taken place, so Cognizant never had an opportunity to investigate or remedy any alleged breach.

[6] While Maritz claims it is entitled to nominal damages, Maritz' conclusory allegation that the sharing of credentials "caused Maritz to suffer damages" (Compl. ¶ 65) is "wholly insufficient as pleading the requisite element of damages." *Scher v. Sindel*, 837 S.W.2d 350, 354 (Mo. Ct. App. 1992).

D. Billing for Time Spent Engaging in Cyberattacks.

Maritz barely responds to Cognizant's arguments that (1) Maritz did not allege that any Cognizant employee plausibly participated in the cyber-attack, and (2) Maritz has not alleged facts to show that Cognizant improperly charged Maritz when it was billed on a set monthly basis. Maritz' only response (in a footnote) is to claim that those arguments go "to the merits." But Maritz does not explain why these issues cannot be decided on a motion to dismiss. Both issues involve the standard inquiry on a motion to dismiss—a claim's plausibility as stated. And Maritz did not, and cannot, object to the Court's consideration of the Statements of Work attached to Cognizant's motion as relevant information in considering whether it is plausible that Maritz would have directly paid improper time charges. *See* Cognizant Mem. 2 n.1 & Def. Exs. A-D.

Maritz also has not pleaded facts plausibly showing that any Cognizant employee engaged in the cyber-attack at all. *See supra* I. Thus, no overbilling has been plausibly alleged. Regardless, Maritz' pleading is also so devoid of *any* details, including basics such as the identity and content of the relevant contractual provisions, that it fails to comply with Rule 8. *See, e.g.*, *Greer v. City of Wichita, Kansas*, No. 16-1185-EFM-JPO, 2017 WL 1492937, at *6 (D. Kan. Apr. 26, 2017) (granting motion to dismiss because the short, plain statement required by Rule 8 "must include, *at the very least*, the existence of contract and the way in which its terms were breached." (emphasis in original)); *Warren v. John Wiley & Sons, Inc.*, 952 F. Supp. 2d 610, 625 (S.D.N.Y. 2013) (dismissing breach of contract claim when plaintiff failed to identify the relevant contracts or "list any of the contract terms").

Maritz does not even identify the relevant Statement of Work—the agreement that includes the schedule for payment—that Cognizant allegedly breached. Conclusory allegations that unknown employees at an unknown time caused Cognizant to overbill in breach of unspecified contract terms are insufficient as a matter of law.

V. The Economic Loss Rule Bars Maritz' Negligence Claim

It is axiomatic that "[t]he mere failure to perform a contract cannot serve as the basis of tort liability for negligence." *State ex rel. William Ranni Assoc., Inc. v. Hartenbach*, 742 S.W.2d 134, 140 (Mo. banc 1987). The duties Cognizant allegedly owed Maritz derive solely from the MSA. Cognizant Mem. 14–15. In opposition, Maritz purports to identify two new duties separate from the MSA: the obligation to "exercise due care in the performance of contract undertakings" and the "duty to prevent foreseeable harm." Maritz Mem. 12–13. But if these duties arise out of something other than the agreement, they then collide with the economic loss rule, which "prohibits a cause of action in tort where the losses are purely economic." *Rockport Pharmacy, Inc. v. Digital Simplistics, Inc.*, 53 F.3d 195, 198 (8th Cir. 1995). Maritz' injuries are economic—it does not claim that it suffered "physical harm" through Cognizant's performance. *Crowder v. Vandendeale*, 564 S.W.2d 879, 882 (Mo. banc 1978). Accordingly, the economic loss rule also bars Maritz' negligence claim. *See, e.g.*, *Trademark Med., LLC v. Birchwood Labs., Inc.*, 22 F. Supp. 3d 998, 1004 (E.D. Mo. 2014) (dismissing plaintiff's tort claim under the economic loss rule, concluding granting leave to amend would be futile).

VI. Maritz Failed to Plead Its Unjust Enrichment Claim in the Alternative.

Cognizant moved to dismiss Maritz' unjust enrichment claim for the same reasons it sought dismissal of Maritz' breach of contract claim regarding improper billing. *See* Cognizant Mem. 15; *supra* I. Cognizant also moved to dismiss Maritz' unjust enrichment claim because Maritz did not truly plead its unjust enrichment claim in the alternative. Cognizant Mem. 15. Maritz argues (at 15) that one court has permitted unjust enrichment claims to proceed even when a party incorporates its breach of contract allegations, but that is against the weight of better-reasoned authorities. *See, e.g.*, *Jacobson Warehouse Co., Inc. v. Schnuck Markets, Inc.*, No. 4:17-CV-00764 JAR, 2017 WL 5885669, at *2 (E.D. Mo. Nov. 29, 2017); *Marks v. Compo Steel Prod., Inc.*, No.

08C5049, 2008 WL 5221172, at *4 (N.D. Ill. Dec. 12, 2008) And beyond Maritz's own pleading failure, the Complaint does not contain "factual allegations" that could lead to a "plausible inference" that Maritz could state an alternative unjust enrichment claim when there is not a single allegation to suggest the MSA could ever be found unenforceable. *Deltacom, Inc. v. Budget Telecom, Inc.*, No. 5:10-CV-38-FL, 2011 WL 2036676, at *6 (E.D.N.C. May 22, 2011). Thus, Maritz' unjust enrichment claim should be dismissed.[7]

CONCLUSION

For the foregoing reasons, and those included in its opening memorandum of law, Cognizant respectfully requests that the Court dismiss the Complaint. Maritz filed this claim only after hiring multiple security firms to pursue significant investigations into the phishing attacks and theft. *See* Compl. ¶¶ 27, 38. Maritz possesses all the facts it has about the cyberattacks. Accordingly, any amendment to Maritz' Complaint is futile, and the case should be dismissed with prejudice. *Pet Quarters, Inc. v. Depository Tr. & Clearing Corp.*, 559 F.3d 772, 782 (8th Cir. 2009)

[7] Maritz is not entitled to an equitable accounting. Maritz misstates the claim's prerequisites by arguing it must only allege "the existence of a relationship of trust." Maritz Mem. 14 n.8. In reality, Maritz must allege that a specified "fiduciary or *trust relationship*" exists. *Eckel v. Eckel*, 540 S.W.3d 476, 488 (Mo. Ct. App. 2018) (emphasis added). Maritz conflates a "trust relationship," *i.e.*, the legal term of art for relationship between a trustee and a legal trust, and the lay meaning of a "relationship of trust." Only the former can trigger an equitable accounting. *See Engelsmann v. Holekamp*, 402 S.W.2d 382, 388 (Mo. 1966) (holding there needed to be "proof of the existence of a fiduciary relationship"; recognizing that trustees "stood in a fiduciary capacity"). Cognizant did not serve as a fiduciary or as a trustee in any capacity for Maritz.

Dated: October 31, 2018

Respectfully submitted,

/s/ *Patrick A. Harvey*
Ronald J. Tenpas*
2200 Pennsylvania Ave. NW
Suite 500 West
Washington, DC 20037
Tel: (202) 639-6791
Fax: (202) 879-8981
E-mail: rtenpas@velaw.com

-and-

Patrick A. Harvey*
MORGAN, LEWIS & BOCKIUS LLP
1111 Pennsylvania Avenue, N.W.
Washington, DC 20004
Phone: (202) 739-3000
Fax: (202) 739-3001
E-mail: patrick.harvey@morganlewis.com

*admitted *pro hac vice*

-and-

Jim Martin
DOWD BENNETT LLP
7733 Forsyth Blvd.
St. Louis, MO 63105
Phone: (314) 889-7300
Fax: (314) 863-2111
Email: jmartin@dowdbennett.com

Counsel for Defendant Cognizant Technology Solutions U.S. Corporation

CERTIFICATE OF SERVICE

I certify that on October 31, 2018 a true copy of the foregoing was served by the ECF e-filing system on the following:

Brian A. Lamping
blamping@thompsoncoburn.com
Jan P. Miller
jmiller@thompsoncoburn.com
Kristen E. Sanocki
ksanocki@thompsoncoburn.com
Thompson Coburn, LLP
One US Bank Plaza
505 N. 7th Street
St. Louis, MO 63101

/s/ *Patrick A. Harvey*
Patrick A. Harvey